Federal Communications Commission
Washington, D.C. 20554

February 23, 2018

VIA ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W., Room TW-B204
Washington, DC 20554

RE: *Ex Parte* Presentation:
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, GN Docket No. 13-111

Dear Ms. Dortch:

Pursuant to Section 1.1206(b) of the Commission's rules, staff are electronically submitting into the record of this proceeding the attached email and presentation sent to me on February 20, 2018, by James Fischer of Cell Command, Inc., discussing the issue of combatting contraband wireless device use in correctional facilities.

Sincerely,

/s/ Charles Mathias

Charles Mathias, Associate Chief
Wireless Telecommunications Bureau
FCC Ombudsperson for Contraband Device Issues

From:	John Fischer <john.fischer@cellcommand.tech>
Sent:	Tuesday, February 20, 2018 3:20 PM
To:	Charles Mathias
Subject:	RE: Thank you
Attachments:	Technology Requirements To Eliminate Contraband Cell Phones voiced from CORRECTIONS, the CARRIERS, and the FCC.pdf

Charles,

Thank you very much for your Feb. 13th email (reprinted below). In response, I have put together a list of requirements that have been strongly voiced and heard over the past decade (many of which were reiterated during the Feb.7th meeting) in what a solution should have to fulfill the requirements of the Corrections industry, the Carriers and the FCC. I would ask anyone receiving this to please add to this list if anything is missing. (list is also attached)

CORRECTIONS REQUIREMENTS:

1. **COMPLETE DEVICE DISABLEMENT**: The system must **COMPLETELY** disable the phone: No TALK, No Text, No Email, No Wifi, No Camera, No Video.[1]
2. **LOW COST:** The system must be affordable so all 7,442 correctional facilities and detention centers in the U.S. can be outfitted.[2]
3. **IMMEDIATE DISABLEMENT**: The system MUST immediately take down the phone upon entering the correctional facility.[3]
4. **ZERO OBSOLESCENCE:** The system must be backward/forward compatible without exception/downtime issues.[4]
5. **NO ADDITIONAL STAFFING REQUIREMENTS**: The system must operate on its own.[5]
6. **Warden/EMT usage:** The system should able to authorize and permit **Warden/EMT usage** of their devices.[6]

CARRIER REQUIREMENTS:

7. **ZERO INTERFERENCE:** The system WILL NOT interfere or molest carrier frequencies or create holes in carrier coverage.[7]
8. **NO CONTINUING STAFF ASSISTANCE**: Set it and forget it. Once up and running, the Carriers will not incur continuing operational staff requirements.[8]

FCC REQUIREMENTS:

9. **LEGAL:** The system must be legal and not violate the 1934 telecommunications act.[10]
10. **Emergency 911 REMAINS OPERABLE:** The system must allow for emergency calling.[11]

IMPORTANT NOTE: Continuous Wave Beacon Technology is the only technology to date that meets each and every one of the above requirements.

Acronyms for footnotes: CWBT – Continuous Wave Beacon Technology. MA – Managed Access. MJ – Micro Jamming. DT – Detect & Locate. IPSP – Inmate Phone System Provider.

[1] *Very important* – CWBT completely disables the device. No other technology completely disables the device. If a Non-IPSP WiFi-internet connection still works, there is a whole in the system. If Camera and Video still work, there is a whole in the system. SD cards can be used to transfer large amounts of information. Escape routes can be mapped out; Terroristic and witness intimation threats can be recorded; Drug drops and outside contact information can be easily passed via the recordable media.

[2] CWBT is 60% - 90% less in cost than MA, MJ, & DT depending on the size of the facility. States do not have excess money in their operating budgets to pay for these technologies. Cell Command has approached the inmate phone system providers to cover the install cost as it is known they will receive great revenue increases from their phone services upon full implementation. Feedback to this idea has been exceptional due to the low cost of CWBT. (Happy to share upon request).

[3] CWBT is the only system that has COMPLETE & IMMEDIATE DEVICE DISABLEMENT. Inmates have learned how defeat M.A. by simply switching sim cards several times throughout the day. Then old sims go out – new sims come in. A system that permits contraband device usage for even a day is not worthy of taxpayer dollars.

[4] CWBT automatically advances forward with all upgrades – the reason is because the technology works on the device and not the Carrier frequency. As we enter 5G and beyond, there must be <u>zero system outages and/or additional costs</u> for upgrade modifications. As 4G-LTE was rolled-out, the Managed Access systems quickly became obsolete requiring massive and expensive overhauls. This happened all over the world with regard to jamming technologies. **NOTE:** MA, MJ and DT technologies will require complete system updates and new testing as technology advances.

[5] CWBT requires zero correctional facility management or staff assistance. Correctional facilities are already short staffed and over worked. Systems that require additional correctional staff to monitor, operate or carry out specific implementation processes and procedures for the technology to work are not preferred. MA & DL both require correctional facility management or staff assistance.

[6] **Note:** CWBT uses a biometric fingerprint password to allow authorized personnel full phone usage. This means an authorized phone in the wrong hands still will not work! A white listed MA phone can easily end up in the hands of an inmate. There is no authorization possible using MJ systems.

[7] CWBT does not touch the carrier frequencies nor does it create any coverage holes. MJ creates frequency interference and creates holes in the Carrier's coverage.

[8] CWBT becomes a set it and forget it technology once the initial migration period is completed. This requirement is voiced because Managed Access requires continuous carrier involvement on several levels.

[9] CWBT is completely legal and it does not violate the 1934 Telecommunications Act. There is great controversy over whether any form of jamming is legal.

[10] NOTE: CWBT provides a 10 second window while the device is shutting down in which 911 will automatically be connected if dialed or the icon is pushed. No form of jamming allows for emergency calling.

If you have any questions, please do not hesitate to call.

Best regards,

John J. Fischer

Chief Executive Officer

CELL COMMAND, INC.
(formerly TRY SAFETY FIRST, INC.)
(770) 652-4517
john.fischer@cellcommand.tech
http://twitter.com/tsfprotocols

From: Charles Mathias [mailto:Charles.Mathias@fcc.gov]
Sent: Tuesday, February 13, 2018 6:34 PM
To: john.fischer@cellcommand.tech
Cc: Roger Noel; Lloyd Coward; Anna Gentry; Melissa Conway; Mary Claire York
Subject: Thank you

Thank you for participating in the fact-finding meeting at the FCC on Wednesday 7 February. We appreciate the wide-ranging and candid discussion about the many issues associated with the contraband phone crisis in correctional institutions across the country. We were encouraged to find consensus throughout the group that increased collaboration between all stakeholders is essential to finding effective and affordable solutions. To that end, we value CTIA's willingness to stand up a forum where representatives from corrections departments will be able to collaborate directly with both wireless carriers and contraband solutions providers to test a variety of technology approaches including MAS, Advanced Detection, and with our federal partners, precision or micro jamming. We also thought the idea of adapting the CTIA/GSMA Stolen Phone Checker to disable contraband devices could be very useful.

We are working with Patrick Donovan at CTIA on next steps and will have more information soon. We hope the discussions will begin as soon as possible and look forward to working with you all.

Charles Mathias
Charles B. Mathias
Associate Bureau Chief/ Ombudsperson for Contrand Device Issues
Federal Communications Commission/Wireless Telecommunications Bureau
202.418.7147

The following people have been BCC'd on this email (bccd in order to keep their email address confidential):

Ajit Pai
Julius Knapp
Melissa Conway
Brendan Carr
Lloyd Coward
Dana Shaffer
Lindsey Freeman
Katherine Crytzer
Roger Noel
Anna Gentry
Mary Claire York

James Basinger
Brian Benison
Milton Brown
Gina Cacciatore
Matthew Caesar
Bryan Collier
Todd Craig
J. David Donahue
Patrick Donovan
Gregory Dozier
Kyle Entz
David Gitttelson
Mark Greene, Ph.D
Eric Hagerson
Pelicia E. Hall
Joseph Heaps
Mark S. Inch
A representative of J3 Technology*
Jessica B. Lyons
Howard Melamed
Jay E. Miller
Robert Morse
Tony C. Parker
Mark Reddish
Ray Rothermel
Sean K. Smith
Joseph Robert Smyjunas Bryan Stirling
Rebecca Murphy Thompson Pete Tomczak
Jim Viscardi
Nicole Zimbelman
Lee Dotson

* Indentity of representative J3 Technology redacted